VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Kvalita služby v sítích LAN

Quality of Service in LAN Networks

2019 Filip Lauterbach

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání bakalářské práce

Student: **Filip Lauterbach**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2601R013 Telekomunikační technika

Téma: Kvalita služby v sítích LAN
Quality of Service in LAN Networks

Jazyk vypracování: čeština

Zásady pro vypracování:

Cílem bakalářské práce je návrh, realizace a testování nástrojů pro podporu kvality služby (QoS) v sítích LAN v laboratorním prostředí s využitím síťových zařízení Huawei a Cisco.

Osnova práce:
1. Popište nástroje pro implementaci kvality služby (QoS) v sítích LAN.
2. Navrhněte a v laboratorních podmínkách realizujte sítě LAN využívající síťová zařízení Huawei a Cisco, v nichž jsou použity alespoň 3 různé nástroje pro podporu QoS. Ověřte funkčnost navržených řešení.
3. Ověřte kompatibilitu síťových zařízení Huawei a Cisco při implementaci těchto nástrojů.
4. Srovnejte možnosti nasazení nástrojů QoS v sítích LAN a WAN.

Seznam doporučené odborné literatury:

[1] ODOM, Wendell. a Michael J. CAVANAUGH. *Cisco QOS exam certification guide*. 2nd ed. Indianapolis, IN: Cisco, 2005. ISBN 978-1-58720-124-0.
[2] SZIGETI, Tim, Christina HATTINGH, Robert BARTON a Kenneth BRILEY. *End-to-end QoS network design*. 2nd edition. Indianapolis, IN: Cisco Press, 2014. Cisco Press networking technology series. ISBN 978-158-7143-694.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Petr Machník, Ph.D.**

Datum zadání: 01.09.2018
Datum odevzdání: 30.04.2019

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA Fakulta elektrotechniky a informatiky IDI6 OSTRAVA

prof. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. Ing. Pavel Brandštetter, CSc.
děkan fakulty

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 21. dubna 2019 ..... Landerbach .....

Rád bych poděkoval Ing. Petru Machníkovi, Ph.D. za odbornou pomoc a konzultaci při vytváření této bakalářské práce.

Abstrakt

Tato bakalářská práce se zabývá popisem a praktickou implementací nástrojů kvality služby na zařízeních od společnosti Huawei a Cisco. Úvodní část práce se věnuje teoretickému popisu kvality služby. Zejména popisem základních parametrů kvality služby, jako je propustnost, zpoždění, variabilita zpoždění a ztrátovost paketů. Následuje popis hlavních nástrojů kvality služby a s nimi souvisejících modelů. V další části je popsáno testování jednotlivých nástrojů na obou zařízeních Huawei i Cisco. Následně je ověřena kompatibilita obou zařízení.

Klíčová slova: Cisco, Huawei, Klasifikace provozu, Kvalita služby, Omezování provozu, Priorizace provozu, Přepínač, Tvarování provozu, Značkování provozu

Abstract

This thesis deals with description and practical implementation of the Quality of service tools on Huawei and Cisco devices. First part of the thesis deals with a theoretical description of Quality of service. Especially, the basic parameters of Quality of service such as bandwidth, delay, jitter and packets loss. In the second part there is a description of the main Quality of service tools and their related models. The next part of thesis describes testing of individual tools on both devices Huawei and Cisco. Final part of my thesis verifies compatibility of both Huawei and Cisco devices.

Key Words: Cisco, Huawei, Quality of Service, Switch, Traffic classification, Traffic marking, Traffic policing, Traffic prioritization, Traffic shaping

Obsah

Seznam použitých zkratek a symbolů

ACL	–	Access Control List
Bc	–	Burst size
Be	–	Excess Burst size
BER	–	Bit Error Rate
CAC	–	Call Admission Control
CBS	–	Commited Burst Size
CBWFQ	–	Class-Based Weighted Fair Queuing
CFI	–	Canonical Format Indicator
CIR	–	Committed Information Rate
CoS	–	Class of Service
CQ	–	Custom Queuing
DiffServ	–	Differentiated Services
DRR	–	Deficit Round Robin
DSCP	–	Differentiated Service Code Point
DSP	–	Digital Signal Processor
EBS	–	Excess Burst Size
FCS	–	Frame Check Sequence
FIFO	–	First In, First Out
ID	–	Identification
IEEE	–	Institute of Electrical and Electronics Engineers
IntServ	–	Integrated Services
IP DA	–	Internet Protocol Destination Address
IP SA	–	Internet Protocol Source Address
LFI	–	Link Fragmentation and Interleaving
LLQ	–	Low Latency Queuing
MAC	–	Media Access Control
MLS	–	MultiLayer Switch
MTD	–	Modified Tail Drop
P2P	–	Peer to Peer
PHB	–	Per Hop Behaviors
PIR	–	Peak Information Rate
PQ	–	Priority Queuing
QoS	–	Quality of Service
RED	–	Random Early Detection
RTP	–	Real-time Transport Protocol
Rx	–	Receiver

SP	–	Strict Priority
SP+DRR	–	Strict Priority + Deficit Round Robin
SP+WRR	–	Strict Priority + Weighted Round Robin
SRR	–	Shaped Round Robin
TCI	–	Tag Control Information
TCP	–	Transmission Control Protocol
ToS	–	Type of Service
TPID	–	Tag Protocol Identifier
TTL	–	Time to live
Tx	–	Transmitter
VLAN	–	Virtual Local Area Network
VoIP	–	Voice over Internet Protocol
VPN	–	Virtual Private Network
WFQ	–	Weighted Fair Queuing
WRR	–	Weighted Round Robin
WTD	–	Weighted Tail Drop

Seznam obrázků

Seznam tabulek

1 Úvod

S velkým rozvojem počtu poskytovaných služeb v rámci počítačových sítí, vznikl problém s garancí kvality těchto služeb. Dřívější klasické počítačové sítě založené na standardu 802.3 (Ethernet), využívající rodinu protokolů IP, nerozlišovaly typ paketů. Pouze se snažily tyto pakety doručit do cílového místa v co nejkratší době tzv. metodou Best Effort. Tato metoda nezaručovala garanci spolehlivé služby.

V moderní době je nutné provoz značkovat a zaručit mu potřebné prostředky, např. online video přenosy vyžadují nízké zpoždění a stabilní přenosovou rychlost. Proto vznikl mechanizmus kvality služby (QoS), díky kterému můžeme datový tok značkovat a pomocí značek tento tok priorizovat před ostatními méně důležitými toky. Hlavními parametry kvality služby jsou propustnost, zpoždění, varibialita zpoždění a ztrátovost paketů.

První část bakalářské práce se věnuje teoretickému popisu kvality služeb. Jsou zde popsány základní parametry a nástroje související s kvalitou služeb.

Druhá část se věnuje praktické realizaci QoS nástrojů na přepínačích obou předních výrobců síťových zařížení a to na zařízeních od firmy Cisco a Huawei. Je testováno značkování a mapování provozu, dále omezování a tvarování provozu a jako poslední priorizace provozu. Tyto nástroje jsou dále porovnány v rámci podobnosti příkazů, tak také v rámci funkčnosti na obou zařízeních předních výrobců.

2 Základní popis Kvality Služby

Kvalita služby neboli QoS (Quality of Service), je řada technologií, která řeší problémy v oblasti propustnosti sítě (traffic management). Oficiální definice podle ITU-T E.800: „Souhrn charakteristik telekomunikační služby, které souvisejí se schopnostmi uspokojovat potřeby uživatele služby.“

Kvalita služby řeší řízení a rezervaci síťových zdrojů v telekomunikačních a počítačových sítích nastavením různých priorit pro konkrétní typy dat (video, audio apod.). Důvodem vzniku QoS je fakt, že počet uživatelů internetu nadále roste a spolu s tím se navyšují také požadavky na výkonnost sítě. Například mnohé z online služeb vyžadují vysoké množství propustnosti (bandwidth) či nízké zpoždění (delay) při přenosu sítí, např. v případě přenosu hlasu (VoIP) přes IP protokol. Proto je nutné priorizovat provoz, tzn. upřednostnit určitý provoz před jiným, omezit propustnost apod.

V dalších podkapitolách bude podrobně vysvětlena problematika QoS, její modely a parametry. [1][2][3][4]

Tabulka 2.1: Chování QoS podle typu provozu

Typ Provozu	**Chování bez použití QoS**
Hlas	Hlas je nesrozumitelný Hlas se rozpadá, není plynulý Zpoždění způsobuje, že účastníci hovoru neví, kdy druhá strana dohovořila Odpojování hovorů
Video	Neplynulý průběh videa Audio není synchronizováno s videem Zpomalený pohyb videa
Data	Pozdní příchod dat Nepravidelné doby odezvy omezují uživatele

2.1 Parametry Kvality Služby

Aplikací QoS nástrojů se nejčastěji ovlivňují tyto následující kvalitativní parametry přenosu:

- Propustnost (Bandwidth)
- Zpoždění (Delay)
- Variabilita zpoždění (Jitter)
- Ztrátovost paketů (Packet Loss)

Nicméně zlepšení jednoho z QoS parametru může degradovat parametr jiný. Propustnost definuje kapacitu přenosového média. Kompresní nástroje snižují celkovou šířku pásma, která je potřeba pro přenesení všech paketů, avšak komprese s sebou nese jisté zpoždění a spotřebovává procesorový výkon. Variabilita zpoždění je zpoždění mezi po sobě jdoucími pakety. Zařízení obvykle může snižovat variabilitu zpoždění pro určitý typ provozu, avšak za cenu vzniku zpoždění nových na ostatních datových provozech. QoS principy řeší zpoždění využitím řazení prvků do front podle priorit. Ztrátovost paketů vzniká důsledkem přenosových chyb, QoS mechanizmy nemají možnosti jak tuto ztrátovost dramaticky ovlivnit.

QoS funkce navíc dokáží ovlivnit, které pakety budou vynechány. Klíč úspěchu v oblasti QoS tkví ve vylepšení charakteristiky pro datové toky, které tuto charakteristiku vyžadují a naopak degradaci stejné charakteristiky pro toky, které tuto vlastnost nepotřebují.

Např. pro optimální využití IP telefonie v dané síti by měla síť splňovat tyto parametry: zpoždění < 150 ms, variabilitu zpoždění < 30 ms a ztrátovost paketů by neměla překročit 1 %. [1][2][3][5]

2.1.1 Propustnost

Propustnost vyjadřuje množství bitů, které jsou přeneseny mezi zařízeními za určitý časový úsek, zpravidla 1 s. V některých případech se může propustnost přímo rovnat fyzické přenosové rychlosti. Avšak v ostatních případech je propustnost menší než skutečná přenosová rychlost. Je to způsobeno tím, že v rámci dvou bodů může být více linek s rozdílnou propustností, potom je propustnost určena nejpomalejší linkou na této trase. [1][2][3]

2.1.1.1 Nástroje ovlivňující šířku pásma

Řešením může být využití tzv. Link-efficiency QoS nástroje, který využívá komprese dat pro snížení počtu přenášených bitů po médiu. Uvedu příklad, máme směrovač R1, který využívá kompresní poměr 2:1. Bez využití kompresní metody s 80kbit/s vnější linkou (příchozí síť) a

pouze 64kbit/s P2P linkou, v síti dojde k vytvoření fronty paketů. Fronta se časem naplní a přebývající pakety se zahodí. Tato metoda se nazývá Tail drop. S využitím komprese s kompresním poměrem 2:1 dojde ke zvýšení propustnosti na dvojnásobek. V opačném případě by došlo ke snížení dat na 64 kbit/s a k zadržování paketů ve frontě. [1][2][3][4]

Exitují i další metody ovlivňující propustnost, první z nich se nazývá CAC (Call Admission Control), tato metoda rozhoduje, zdali bude povolen další video popř. hlasový hovor z důvodu zachování kvality hovorů. Např. v návrhu může být povolen např. omezený počet hovorů. Druhá metoda se jmenuje Queuing, tato metoda vytváří větší množství front, ze kterých jsou poté vybírány pakety na základě určitého algoritmu. Lze tedy nadefinovat minimální velikost propustnosti pro různé druhy paketů. [1][2][3][4]

2.1.2 Zpoždění

Druhým parametrem, díky kterému můžeme ovlivňovat QoS v síti je zpoždění. Existuje více druhů zpoždění.

Zpoždění serializace (Serialization delay) vyjadřuje čas, který je nutný pro zakódování bitů zprávy na fyzickou vrstvu. Toto zpoždění je fixní a lze ho popsat rovnicí:

$$zpoždění\ serializace = \frac{počet\ odeslaných\ bitů}{rychlost\ linky} \tag{1}$$

Zpoždění propagace (Propagation delay) vyjadřuje čas, který trvá jednomu bitu dostat se z jednoho konce linky na druhý. Toto zpoždění je fixní a lze ho popsat rovnicí:

$$zpoždění\ propagace = \frac{délka\ linky\ [m]}{2.1 \cdot 10^8\ [m/s]} \tag{2}$$

Zpoždění na frontách (Queuing delay) je zpoždění způsobené na zařízení. Zpoždění způsobené čekáním než další pakety mohou být odeslány. Je to čas, který stráví paket ve frontách na zařízení. Předchozí dvě zmiňované zpoždění se posléze k tomuto zpoždění přičítají. Toto zpoždění je variabilní.

Zpoždění přesměrování (Forwarding delay) je čas, který stráví paket na zařízení. Je to délka trvání mezi prozkoumáním paketu/rámce ze vstupu a vložení ho do odchozí fronty na výstupní port. Tento čas nezahrnuje čas strávený ve frontě (queuing delay), toto zpoždění je variabilní.

Tvarovací zpoždění (Shaping delay) je závislé na rychlosti obsluhy jednotlivých front. Můžeme zvolit pomalejší posílání paketů a využít rychlejší obsluhu jednotlivých front. Při rych-

lém odesílání paketů by velmi pravděpodobně došlo časem k zahození paketů. Toto zpoždění je stejně jako předchozí zpoždění variabilní.

Zpoždění při zpracování paketu síťovým zařízením (Network delay) je typ zpoždění, které vzniká v síti, do které my nemáme přístup např. sítě jiného poskytovatele internetu apod. Je to celkové zpoždění na aktivních prvcích, ke kterým nemáme přístup. Uvedeme si příklad, pokud využíváme nějakou službu, např. cloud, kde na aktivních prvcích vzniká určité zpoždění, tak my jako uživatelé nejsme schopni tyto QoS praktiky na těchto prvcích v cloudu kontrolovat. A z tohoto důvodu nemůžeme toto zpoždění nijak ovlivnit. Toto zpoždění je variabilní.

Zpoždění kodéru (Codec delay) je zpoždění vzniklé potřebným časem na zpracování příchozího analogového signálu a následnou konverzi tohoto signálu na signál digitální a také vlastností zvanou Look-ahead. Existuje mnoho druhů kodeků s rozdílnými časy na zpracování, např. kodek G.729 má zpoždění při zpracování analogového hlasu zhruba 10 ms. Avšak kódovací algoritmus může způsobovat další nadbytečné zpoždění při využití vlastnosti Look-ahead. Look-ahead neboli v překladu „nahlédnutí dopředu“ nastává, pokud je kodek prediktivní.

Tato metoda využívá méně bitů pro zakódování hlasu, což je výhoda. Využívá se vlastnosti lidského hlasu, jelikož hlasivky nedokážou okamžitě přecházet z jednoho zvuku na zdaleka jiný rozdílný zvuk, proto tyto kodeky mohou využívat menší počet bitů pro kódování. Nicméně tyto algoritmy potřebují ke své správné funkci vzorek hlasu pro zakódování a ještě následných několik milisekund hlasu pro predikci. Např. pro zakódování 10ms hlasového vzorku kodekem G.729 potřebujeme ještě 5 ms následujícího vzorku. Toto zpoždění je fixní.

Zpoždění komprese (Compression delay) je zpoždění vznikající při kompresi/dekompresi paketů, také se jedná o variabilní zpoždění. [1][2][3][4]

2.1.2.1 Nástroje ovlivňující zpoždění

Nejznámější QoS nástroj ovlivňující zpoždění je Queuing (Scheduling). Jedná se o nástroj, který pracuje s frontami. Tento nástroj může využívat více front. Nicméně tento nástroj nesnižuje zpoždění pro všechny pakety, ale může zajistit snížení zpoždění pro pakety citlivé na zpoždění (prioritní pakety). A tím pádem zvýšit zpoždění pro pakety, které nejsou prioritní a toto zpoždění jim neuškodí.

Druhým nástrojem je Link Fragmentation and Interleaving (LFI). LFI vyjadřuje čas potřebný k serializaci paketu na médium. Pokud směrovač začne odesílat postupně bity z paketu, musí tento paket celý odeslat. Může však nastat situace, že v danou chvíli dorazí paket citlivý na zpoždění a ten nemůže být odeslán do doby, než bude odeslán kompletně celý už odesílaný paket. Což by mohlo být v mnoha případech nepřípustné, např. využití VoIP či streamingu. Proto nástroj LFI využívá možnosti fragmentace, kdy paket, který není prioritní, rozdělí postupně na

několik částí (fragmentů), směrovač odešle první fragment a vzápětí může odeslat již prioritní paket. Nevzniká tak velké nežádoucí zpoždění.

Třetím nástrojem je komprese. Komprese je využita na paket popř. paketové záhlaví a data jsou zkomprimována, např. 1500bytový paket může být zkomprimován pouze na velikost 750 bytů a tím pádem využít pouze skoro polovinu času serializace oproti variantě bez komprese.

Posledním nástrojem je nástroj Traffic Shaping, který navyšuje zpoždění ve snaze redukovat ztrátovost paketů. [1][2][3][4]

2.1.3 Proměnlivost zpoždění

Jitter je dalším parametrem QoS, který vyjadřuje proměnlivé zpoždění. Proměnlivé zpoždění vzniká na prvcích sítě, pro běžná data není toto zpoždění kritické. Avšak např. digitalizovaný hlas vyžaduje, aby jednotlivé hlasové pakety byly odesílány v pevných intervalech např. 20 ms. Pak by tedy měli pakety dorazit do cíle se stejnými časovými mezerami, tento typ přenosu se jmenuje izochronní přenos. Jitter lze také definovat jako odchylku v rychlosti příchodu (tj. změna zpoždění v síti) paketů, které byly vysílány jednotným způsobem. [1][2][4]

2.1.3.1 Nástroje ovlivňující proměnlivost zpoždění

Zde jsou nástroje stejné jako v předchozím parametru zpoždění. Zpoždění a proměnlivost zpoždění (jitter) jsou podobné parametry, proto je tento parametr ovlivněn stejnými parametry a to těmito: Queing (frontizace), Link fragmentation and interleaving (fragmentace a prokládání paketů), komprese paketů a Traffic shaping, který se snaží zamezit zahazování paketů. [1][2][4]

2.1.4 Ztrátovost paketů

Posledním parametrem QoS je ztrátovost paketů. Směrovače zahazují pakety z mnoha důvodů např. kvůli poškození paketu. Případné poškození paketu, způsobené při přenosu, může být zařízením zjištěno pomocí propočtu kontrolního součtu (FCS). Pakety mohou být ztraceny z důvodu přenosu nebo díky přeplnění front na zařízeních. Nicméně QoS nástroje dokáží snížit vliv ztrátovosti paketů, pouze v případě, kdy je tato ztrátovost způsobena z důvodu plných front. Dnešní přenosová média jsou spolehlivá, tudíž zde dochází ke ztrátám paketů pouze v malém množství, většinou z důvodu bitových chyb (Bit Error Rate = BER), v moderních sítích je hodnota BER $= 10^{-9}$.

VoIP komunikaci minimální ztrátovost nevadí, srozumitelnost hovoru je zachována. Cisco využívá DSP (Digital Signal Processor) procesory, které dokáží částečně nahradit chybějící vzorek hlasu. [1][2][3][4]

2.1.4.1 Nástroje ovlivňující ztrátovost paketů

Jako nástroj ovlivňující ztrátovost paketů se zde uplatňuje nástroj Queuing a Random Early Detection (RED). Queuing zvětšuje paketové fronty a tím zabraňuje častějšímu zahazování paketů. RED nástroj pracuje s předpokladem, že velikost okna TCP komunikace může být zmenšeno v případě ztrátovosti dat. RED zahodí část paketů, aby předcházel přeplnění front a následného zahazování paketů. Tím dojde ke snížení velikosti okna TCP komunikace. TCP komunikace se částečně zpomalí a dojde ke zmenšení rychlosti kvůli častějšímu potvrzování dat. Tato metoda nezabraňuje ztrátám paketů, ale pouze se snaží předcházet stavu plných front. [1][2]

2.2 Nástroje pro modely Kvality Služby

Existují tři modely. Diffserv (Differentiated Services), dále IntServ (Integrated Services) a Best Effort model, který nevyužívá QoS praktiky.

V této kapitole budou popsány jednotlivé vlastnosti, které jsou využívány dvěma hlavními QoS modely a to: Differentiated services (DiffServ) a Integrated services (IntServ).

2.2.1 Klasifikace a značkování provozu

Tento nástroj používá klasifikaci paketů/rámců podle určitých vlastností. Směrovač/přepínač musí rozpoznat neboli klasifikovat, o jaký typ paketu se jedná, např. o RTP pakety pro VoIP služby nebo pouze o datové pakety. Klasifikace do jednotlivých tříd většinou probíhá zjištěním informací z hlaviček paketů/rámců, díky této vlastnosti můžeme dále označit a priorizovat tento provoz před ostatním ne tak důležitým provozem.

Na aktivním prvku jsou nastavena určitá pravidla, a podle toho jakému pravidlu daný typ provozu odpovídá je paket zařazen do příslušné fronty, která obsahuje pakety se stejnými potřebami.

Provoz na L2 vrstvě ISO/OSI modelu se kategorizuje do jednotlivých tříd pomocí pole (CoS - Class of Service) v hlavičce rámce 802.1Q. IEEE 802.1Q je standard, nazýván také VLAN Tagging, jelikož umožňuje rozdělit fyzickou Ethernetovou síť na větší počet logických sítí tzv. VLAN. Oproti běžnému Ethernetovému rámci má hlavička rámce 802.1Q navíc již zmíněnou položku CoS. Tato položka definuje osm tříd. [1][2][6][7]

Tabulka 2.2: 802.1Q Ethernet rámec

6B	**6B**	**4B**	**2B**	**64 - 1500B**	**4B**
Cílová adresa	Zdrojová adresa	802.1Q tag	Typ nebo Délka	Data	FCS

Cílová adresa: Obsahuje unikátní 48bitovou MAC adresu v hexadecimálním tvaru XX:XX:XX:XX:XX:XX, kde X zastupuje jeden hexadecimální znak, využívá se k adresování cílového zařízení na L2 vrstvě ISO/OSI modelu.

Zdrojová adresa: Obsahuje taktéž unikátní 48bitovou MAC adresu v hexadecimálním tvaru, využívá se k adresování zdrojového zařízení na L2 vrstvě ISO/OSI modelu.

802.1Q tag: Pole se využívá pro označení čísla VLAN a označení priority rámce pro využití QoS (jedná se o 3b pole priority s hodnotami od 0 až 7).

Typ nebo Délka: Hodnoty 1500 dekadicky a menší indikují, že se jedná o délku datového pole. Zatímco hodnoty 1536 a větší indikují, že hodnota vyjadřuje EtherType[1].

Data: Obsahuje samotná data vyšší vrstvy.

FCS (Frame Check Sequence): Jedná se o cyklický součet, slouží k detekci poškození rámce.

Tabulka 2.3: 802.1Q tag

16b	**3b**	**1b**	**12b**
VLAN Protocol ID	Priorita (802.1P)	CFI	VLAN ID

VLAN Protocol ID: Obsahuje hexadecimální hodnotu 0x8100, která vyjadřuje takzvaný identifikátor typu rámce. Tento identifikátor zařízení sděluje, že následující dva oktety nesou informace o VLAN.

Priorita (CoS): Obsahuje tříbitovou hodnotu priority rámce, podle které je následně rámec zařazen do odpovídající fronty.

CFI (Canonical Format Indicator): Určuje v jakém pořadí je přenášen rámec (Big Endian/Little Endian), u Ethernetu je využíván Little Endian.

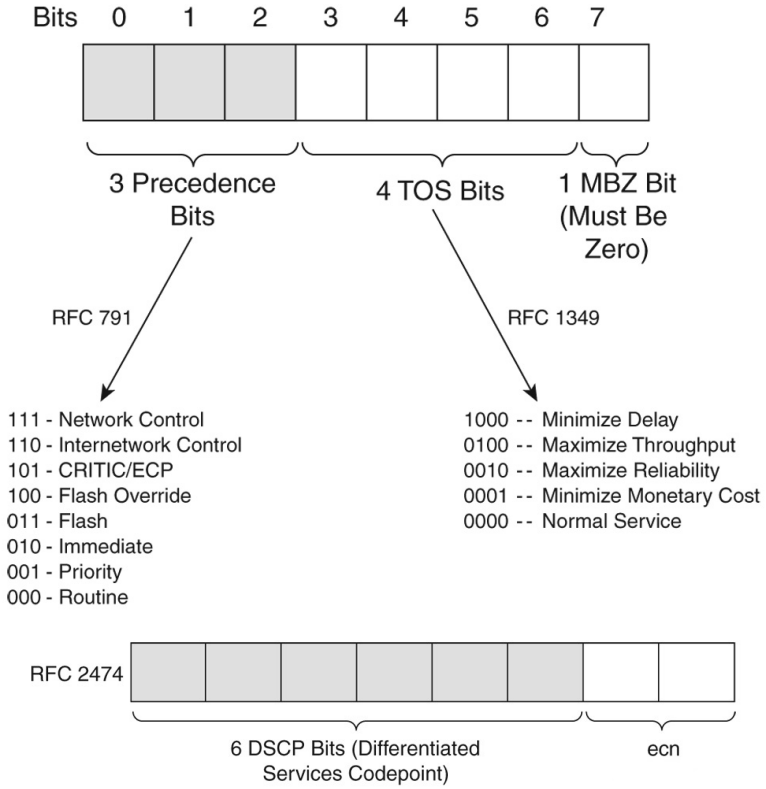
VLAN Identifier: Je identifikace VLANy, jedná se o dvanáctibitové číslo. Máme možnost využít až 4096 VLAN.

Provoz na L3 vrstvě ISO/OSI se kategorizuje podle pole DiffServ v hlavičce IP paketu. DiffServ pole má velikost 8 bitů. Pro využití QoSu je pro nás důležité pole DSCP (Differentiated Service Code Point) s velikostí 6 bitů (hodnoty 0 až 63). V minulosti se využívalo pole Precedence, kvůli DiffServ modelu bylo pole ToS přetvořeno na šestibitové pole DSCP. DSCP umožňuje klasifikovat provoz až do 64 tříd. [1][2][3][6][8]

[1]EtherType indikuje typ protokolu, který je zapouzdřený v datovém poli rámce (IPv4 apod.)

Tabulka 2.4: IP hlavička paketu

4b	**4b**	**8b**	**16b**	**16b**	**3b**	**13b**	**8b**	**8b**	**16b**	**32b**	**32b**	
Verze	Velikost hlavičky	ToS	Délka	ID	Flags	Offset	TTL	Protokol	FCS	IP SA	IP DA	Data



Obrázek 2.1: Schéma TOS a DiffServ pole [9]

2.2.2 Metody obsluhy paketových front

Tato oblast souvisí s DiffServ modelem, který bude popsán v další kapitole. Každé jednotlivé rozhraní má hardwarovou (fyzickou) frontu typu FIFO, zařízení využívají také softwarové fronty, u kterých můžeme využít aplikaci některých typů front, které budou popsány níže.

Pokud linky, na které mají být zařízeními směrovány pakety různých tříd provozu, nejsou zcela vytíženy, není potřeba využívat mechanismy QoS, protože by to vedlo ke zbytečné režii[2] . V tomto případě by pakety byly na linky odesílány pravidlem FIFO (First In-First Out). Avšak v případě, že se začíná plnit výstupní fronta či fronty některých linek, musí zařízení využít

[2]Kromě mechanismu Link Fragmentation & Interleaving

algoritmy, které dále určí, který z paketů bude dále vybrán a odeslán na výstupní linku.

Priorizace provozu se realizuje využitím více front a využitím vhodného režimu obsluhy těchto front. Nejčastější režimy obsluhy front:

- Priority Queuing (PQ)
- Custom Queuing (CQ)
- Weighted Fair Queuing (WFQ)
- Class-Based Weighted Fair Queueing (CBWFQ)
- Low Latency Queuing (LLQ)

Priority Queuing (PQ) podporuje využití až 4 front, fronty mají absolutní priority. Fronty mohou mít různou úroveň priority, nejprve se vybírají pakety z front s vyšší prioritou a až pak následně z front s prioritou nižší. Nevýhodou přístupu PQ je možnost, že k datům ve frontách s nižší prioritou nemusí dlouho dojít z důvodu mnoha dat s prioritou vyšší.

Custom Queuing (CQ) podporuje využití až 16 front, pakety se střídavě (cyklicky) odebírají ze všech front, tak aby byla proporcionálně přidělena kapacita každé třídě provozu.

Weighted Fair Queuing (WFQ) podporuje využití až 4096 front. U této metody jsou pakety toků dynamicky zařazeny do front a tyto fronty jsou dále obsluhovány. Datové toky jsou určeny protokolem 4. vrsty, IP adresami a porty 4. vrstvy. Zařízení preferuje kratší pakety, což vede k preferenci interaktivního provozu. Přidělování podílu pásma závisí na hodnotě DSCP v paketech jednotlivých toků.

Class-Based Weighted Fair Queuing (CBWFQ) Umožňuje využívat až 64 tříd. Lze nastavit propustnost jednotlivým třídám provozu. V případě zahlcení fronty se využívá Tail Drop, popř. vlastnost WRED.

Low Latency Queuing (LLQ) má podobné charakteristiky jako WFQ, avšak nabízí další prioritní frontu. V praxi nejvíce používaná. [1][4][7]

2.2.3 Omezování a tvarování provozu

Tato oblast souvisí se dvěma nástroji Policing a Shaping. Oba dělají to samé, ale jiným způsobem. Jejich účelem je omezit propustnost provozu pomocí nastavení maximálního datového toku.

První nástroj provoz omezuje, tak, že pakety, které by překročili pásmo, přímo zahodí nebo je přeznačkuje. Provoz se může omezovat na vstupu i výstupu z rozhraní.

Druhý nástroj zařazuje pakety do fronty, využívá vlastnosti, že tok je nárazový. Tudíž je tok nástrojem rozložen do delšího času. Může provoz upravovat na výstupu z rozhraní. [4][7]

2.3 Modely Kvality Služby

2.3.1 Differentiated Services

V dnešní době nejvíce využívaný QoS model. Tento model odstraňuje základní problémy IntServ modelu v podobě lepší škálovatelnosti. Negativem je pouze na rozdíl od IntServ modelu negarantování doby doručení, nedochází zde k rezervaci a dohodnutí parametrů před přenosem.

Využívá značkování provozu do jednotlivých tříd na vstupních a výstupních zařízení v síti (hranová zařízení). Díky tomu, už vnitřní prvky nemusí řešit značkování provozu a pouze využijí funkci PHB (Per Hop Behaviors). Tato metoda určuje chování paketu podle třídy jakou je označen. [1][4][6][7]

2.3.2 Integrated Services

Tento model funguje na principu vyjednání rezervaci cesty a dohodnutí na parametrech přenosu před zahájením daného přenosu. Vyjednává se přenosová rychlost, maximální zpoždění apod. Využíval se v sítích s přepojováním okruhů. Tento model nebute v této práci využit. [1][6]

3 Testování Kvality Služby

Následující část této práce bude věnována praktické realizaci QoS nástrojů. Na začátek zde bude představen zátěžový generátor/analyzátor Spirent TestCenter C1. Dále se práce zabývá praktickým využitím QoS nástrojů v laboratoři Katedry telekomunikační techniky. Zde jsou k dispozici tyto varianty zařízení Cisco S2960C/C3650x a Huawei Quidway S2326TP/S5328C. Používané operační systémy jsou 12.2 SE10 (S2960C), 16.3.5b (C3650x) pro zařízení Cisco a 5.70 (S2326TP), 5.150 (S5328C) pro zařízení typu Huawei.

3.1 Zátěžový generátor a analyzátor provozu Spirent TestCenter C1

Pro měření datového provozu využiji zátěžový generátor a analyzátor Spirent TestCenter C1. Přístroj umožňuje generovat a testovat provoz na vrstvách L2–L7. Umožňuje celou škálu generování provozu. Zařízení je vybaveno také grafickým výstupem pro využití síťového softwaru pro testování.

Simulátor obsahuje čtyři 1000 BASE-T metalické porty. Pro testování Kvality Služby bude využita především L2 vrstva. V rámci funkčnosti zařízení lze generovaná data zachytávat ve formátu .pcap a dále je zkoumat např. pomocí softwarového analyzátoru Wireshark. Výsledky se ukládají do sql lite databáze. Tyto výsledky lze v dodávaném softwaru Spirent Reporter uložit ve formátu CSV, PDF nebo HTML. V rámci mé práce bude využita pouze funkčnost L2 a L3 vrstvy ISO/OSI modelu. L3 vrstvu využiji z důvodu potřeby IP hlaviček obsahujících DSCP pole.

Ze zařízení lze generovat výsledky, v rámci těchto výsledků je nutno specifikovat, jaké informační pole mají výsledky obsahovat. Základní výsledkové soubory budou přiloženy v rámci každé kapitoly pro testování daného nástroje. Další výsledky, např. detailnější výpisy budou přiloženy v příloze této práce. Přílohy budou také obsahovat konfigurační soubory jednotlivých přepínačů s vyznačeným důležitým nastavením.

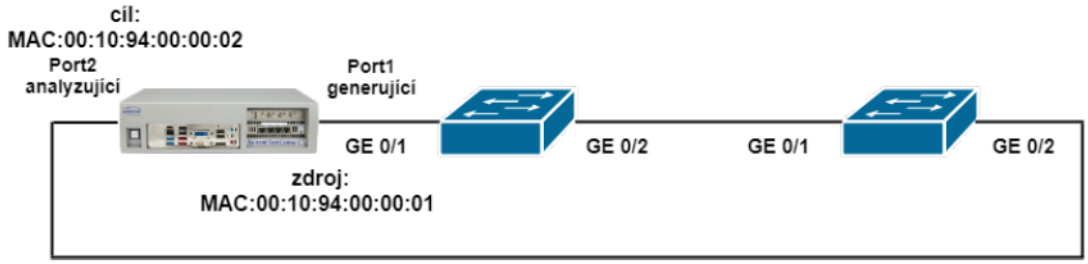
V rámci testování jsou pro nás důležitá pole **L1 Rx Rate (bit/s)** a **L1 Tx Rate (bit/s)**, které udávají přenosové rychlosti vztažené k jednotlivým portům zařízení.

Obrázek 3.1: Zařízení Spirent TestCenter C1 [10]

4 Praktická realizace přeznačkování a mapování provozu

Jako první nástroj pro praktickou realizaci jsem vybral nástroj pro přeznačkování provozu a nástroj pro mapování provozu. Oba nástroje dělají totéž, avšak nástroj pro přeznačkování provozu dává na výběr více možností škálovatelnosti nastavení.

Zvolil jsem jednoduchou topologii se dvěma přepínači. Přepínače jsem propojoval přes gigabitové porty, kvůli generování, co největších datových toků a následného testování.



Obrázek 4.1: Obecná základní topologie přepínačů

4.1 Přeznačkování provozu

4.1.1 Nastavení přeznačkování provozu na přepínačích Cisco

Povolení funkčnosti základních QoS příkazů na přepínači od firmy Cisco se provede pomocí příkazu *mls qos*. Zkratka MLS označuje MultiLayer Switch. Tento příkaz umožňuje využití rozšířených vlastností, mimo jiné například podporu DiffServ QoS. Toto nastavení QoS je na přepínači defaultně vypnuté.

Zapojení obsahuje již v úvodu zmíněné přepínače S2960C od firmy Cisco. Na vstupním portu gigabitEthernet 0/1 prvního přepínače jsou nastavena QoS pravidla. Na začátku je potřeba provoz klasifikovat.

Zařízení Spirent TestCenter C1 již generované datové toky značkuje zvolenými DSCP hodnotami AF12, AF13 a EF (12, 14 , 46 DEC). V této konfiguraci je potřeba zvolit provoz, který bude přeznačkován na jinou hodnotu DSCP. Kritérium pro přeznačkování provozu jsou zde uvedené hodnoty AF12, AF13 a EF. Na každém rozhraní je nutno navíc povolit důvěru v DSCP hodnoty. [11][12]

```
SW1(config)#interface gigabitEthernet 0/1
SW1(config-if)#mls qos trust dscp
SW1(config)#interface gigabitEthernet 0/2
SW1(config-if)#mls qos trust dscp

SW1(config)#class-map Trida1
SW1(config-cmap)#match ip dscp af12 af13 ef
```

Dále je potřeba vytvořit politiku provozu pro danou třídu. Zde je nastaveno přeznačkování provozu. Provozy s DSCP hodnotami AF12, AF13 a EF budou přeznačkovány na hodnotu AF23 (22 DEC). Dále je politika aplikovaná na vstup rozhraní gigabitEthernet 0/1.

```
SW1(config)#policy-map Politika1
SW1(config-pmap)#class Trida1
SW1(config-pmap-c)#set dscp af23

SW1(config)#interface gigabitEthernet 0/1
SW1(config-if)#service-policy input Politika1
SW1(config-if)#mls qos trust dscp

SW2(config)#interface gigabitEthernet 0/2
SW2(config-if)#mls qos trust dscp
```

Dále je k dispozici možnost v rámci politiky nastavit případné zahazování či přeznačkování provozu pomocí příkazu.

```
police rate-bps burst-size [exceed-action {drop | police-dscp-transmit}]
```

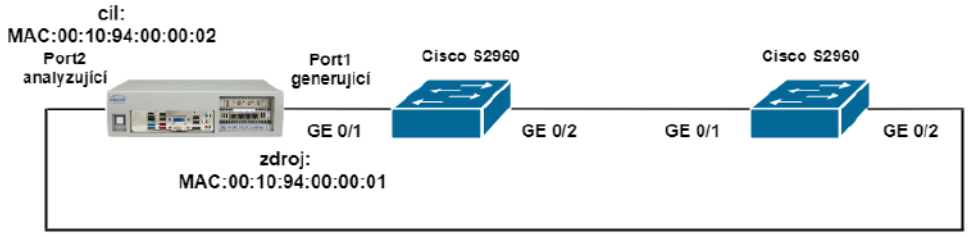
Bohužel L2 přepínač Cisco S2960C na rozdíl od směrovače či L3 přepínače C3650x neumožňuje využití příkazu *shape* pro omezení propustnosti provozu v rámci přeznačkování paketů. Nastavení jsem v omezené podobě využil na vstupním portu gigabitEthernet 0/1 druhého přepínače. Pokud dojde k překročení alespoň jedné nastavené hodnoty v příkazu *police-dscp-transmit*, přepínač automaticky mění hodnotu DSCP na nejnižší možnou a to 0x00 (0 DEC), viz. výpis provozu z programu Wireshark 4.5 v následující kapitole. [6][12]

```
SW2(config)#class-map Trida2
SW2(config)#policy-map Politika2
SW2(config-pmap)#class Trida2
SW2(config-pmap-c)#police 5000000 8000 exceed-action policed-dscp-transmit

SW2(config)#interface gigabitEthernet 0/1
SW2(config-if)#service-policy input Politika2
```

4.1.2 Testování přeznačkování provozu na přepínačích Cisco

Jako výchozí topologii pro testování provozu jsem využil topologii s přidaným rozbočovačem z důvodu sledování procházejícího provozu mezi přepínači. Rozbočovač byl využit jen při kontrole přeznačkování a mapování, při skutečném testování již nebude v dalších kapitolách využit z důvodu co nejlepších přenosových vlastností.

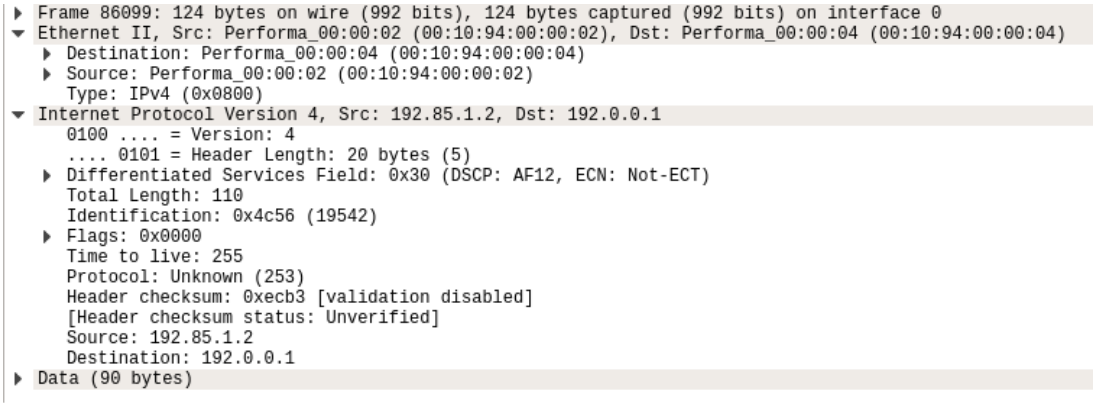
Do sítě byly zařízením Spirent TestCenter C1 generovány značkované datové provozy s DSCP hodnotami AF12, AF13 a EF. Port1 testovacího zařízení byl zapojen do prvního přepínače a port2 byl zapojen na konec sítě za druhý přepínač. Tak jak je znázorněno v testovací topologii. Port1 byl nastaven jako generující a port2 byl nastaven jako analyzující.



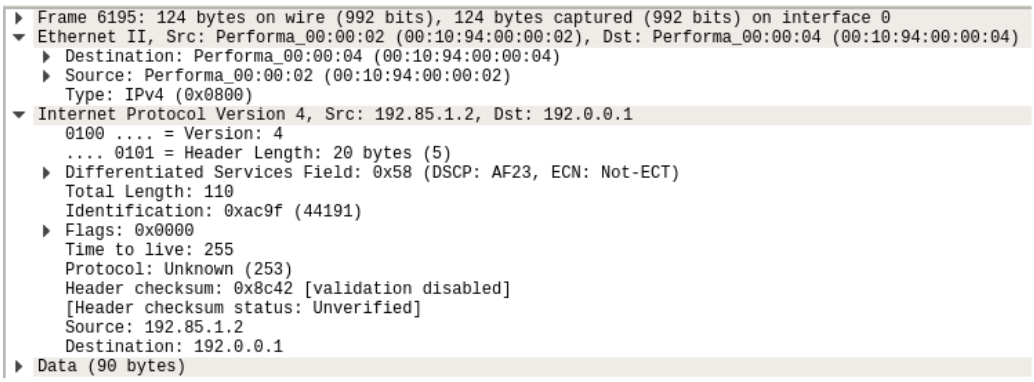
Obrázek 4.2: Cisco testovací topologie pro značkování a mapování provozu

Níže je uveden výpis z programu Wireshark, který ověřuje funkčnost přeznačkování provozů z DSCP hodnot AF12, AF13 a EF na hodnotu AF23. Níže je přiloženo ověření jednoho ze tří generovaných datových toků a to tok s DSCP hodnotou AF12.

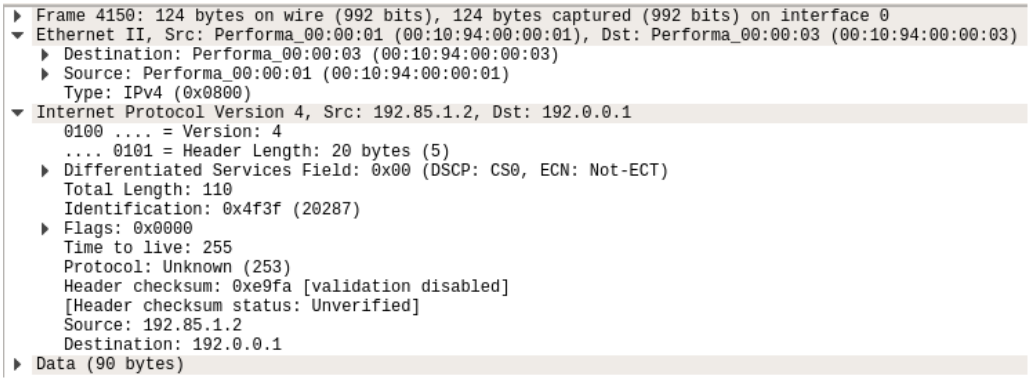
Dále je uveden výpis, který ověřuje funkčnost příkazu *police* s argumentem *policed-dscp-transmit*. Každý provoz byl přeznačkován na nejnižší možnou hodnotu a to CS0.



Obrázek 4.3: Výpis generovaného provozu, AF12



Obrázek 4.4: Výpis přeznačkovaného provozu, AF23



Obrázek 4.5: Výpis přeznačkovaného provozu s DSCP: CS0

4.1.3 Nastavení přeznačkování provozu na přepínačích Huawei

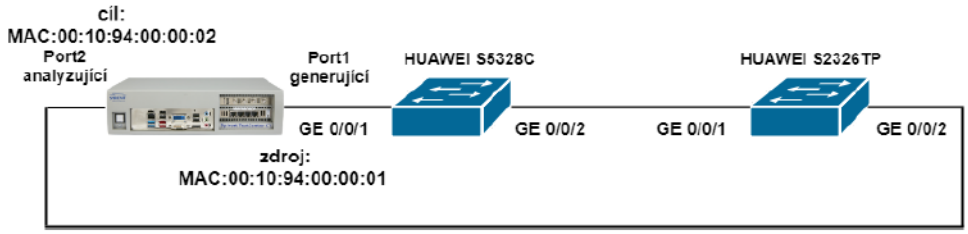
Povolení funkčnosti základních QoS příkazů je již na přepínači Huawei ve výchozím nastavení defaultně zapnuto. Musí se pouze stejně jako na přepínačích Cisco zapnout důvěra v DSCP hodnoty (pro model S5328C).

Nastavení začíná vytvořením třídy, ve které je nutno specifikovat vybraný provoz. Dále je nutno určit jak se bude provoz chovat. Nastavím přeznačkování provozu na AF23. Bude zde využito totožné zapojení jako v případě přepínačů značky Cisco. [13]

```
[SW1]interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet 0/0/1]trust dscp
[SW1]interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet 0/0/2]trust dscp

[SW1]traffic classifier Trida1
[SW1-classifier-Trida1]if-match dscp af12 af13 ef

[SW1]traffic behavior Chov1
[SW1-behavior-Chov1]remark dscp af23

[SW1]traffic policy Politika1
[SW1-trafficpolicy-Politika1]classifier Trida1 behavior Chov1

[SW1]interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet 0/0/1]traffic-policy Politika1 inbound
```

4.1.4 Testování přeznačkování provozu na přepínačích Huawei

Byla využita stejná topologie zapojení jako v případě přepínačů Cisco.



Obrázek 4.6: Huawei testovací topologie pro značkování a mapování provozu

Níže je uveden výpis z programu Wireshark, který ověřuje funkčnost přeznačkování provozů z DSCP hodnot AF12, AF13 a EF na hodnotu AF23.

```
▸ Frame 86099: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0
▾ Ethernet II, Src: Performa_00:00:02 (00:10:94:00:00:02), Dst: Performa_00:00:04 (00:10:94:00:00:04)
  ▸ Destination: Performa_00:00:04 (00:10:94:00:00:04)
  ▸ Source: Performa_00:00:02 (00:10:94:00:00:02)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 192.85.1.2, Dst: 192.0.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x30 (DSCP: AF12, ECN: Not-ECT)
    Total Length: 110
    Identification: 0x4c56 (19542)
  ▸ Flags: 0x0000
    Time to live: 255
    Protocol: Unknown (253)
    Header checksum: 0xecb3 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.85.1.2
    Destination: 192.0.0.1
▸ Data (90 bytes)
```

Obrázek 4.7: Výpis generovaného provozu, AF12

```
▸ Frame 47644: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0
▾ Ethernet II, Src: Performa_00:00:02 (00:10:94:00:00:02), Dst: Performa_00:00:04 (00:10:94:00:00:04)
  ▸ Destination: Performa_00:00:04 (00:10:94:00:00:04)
  ▸ Source: Performa_00:00:02 (00:10:94:00:00:02)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 192.85.1.2, Dst: 192.0.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x58 (DSCP: AF23, ECN: Not-ECT)
    Total Length: 110
    Identification: 0x21b9 (8633)
  ▸ Flags: 0x0000
    Time to live: 255
    Protocol: Unknown (253)
    Header checksum: 0x1729 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.85.1.2
    Destination: 192.0.0.1
▸ Data (90 bytes)
```

Obrázek 4.8: Výpis přeznačkovaného provozu, AF23

4.2 Mapování provozu

4.2.1 Nastavení mapování provozu na přepínačích Cisco

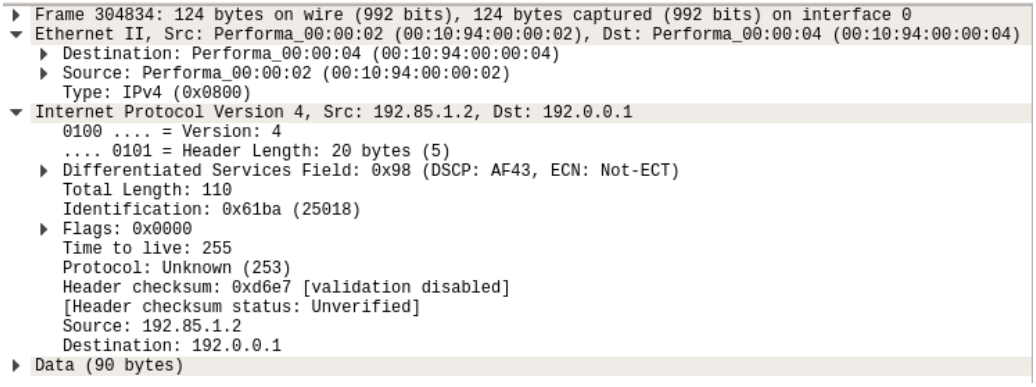
Dále přepínač nabízí k dispozici jednodušší nástroj na konfiguraci přeznačkování provozu. Jmenuje se mapování provozu. Zařízení má více mapovacích tabulek: např. CoS-DSCP, DSCP-CoS, Policed-DSCP, DSCP-mutation atd. Já využiji DSCP-mutation mapu, která umožňuje přemapovat původní DSCP hodnotu či hodnoty oddělené mezarami na odlišnou DSCP hodnotu. Ve výchozím stavu je přemapování ve stavu null, tzn. nemění DSCP hodnoty. Použiji příkaz *mls qos map dscp-mutation WORD 0 to 38* spolu s příkazem *mls qos dscp-mutation WORD* na rozhraní, kvůli přepsání DSCP hodnoty. [6][12]

```
SW2(config)#mls qos map dscp-mutation DSCPmutace 0 to 38

SW2(config)#interface gigabitEthernet 0/1
SW2(config-if)#mls qos trust dscp
SW2(config-if)#mls qos dscp-mutation DSCPmutace
```

4.2.2 Testování mapování na přepínačích Cisco

```
SW2#show mls qos maps dscp-mutation DSCPmutace
   Dscp-dscp mutation map:
   DSCPmutace:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ----------------------------------------
      0 :    38 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63
```

Obrázek 4.9: Výpis příkazu mls qos maps pro mapování provozu s využitím dscp-mutation mapy



Obrázek 4.10: Výpis přeznačkovaného provozu s DSCP: AF43 pomocí dscp-mutation mapy

4.2.3 Nastavení mapování provozu na přepínačích Huawei

Stejně jako v případě přepínačů od firmy Cisco i zde je možnost provoz různě mapovat. Konfigurace je velmi triviální. Mapování se zapne pomocí příkazu:

```
qos map-table {dscp-dot1p | dscp-dp (drop) | dscp-dscp | ip-pre-dot1p | ip-pre-ip-pre}
```

Jako i na předchozím přepínači Cisco i zde je k dispozici více možností namapování, např. pomocí 802.1p priorit (VLAN priorit). Já využiji možnost dscp-dscp mapování. [14]

```
[SW1]qos map-table dscp-dscp
[SW1-maptbl-dscp-dscp]input 0 output 38
```

Prvním číslem za slovem *input* se definuje jaká hodnota DSCP bude měněna. Příkaz umožňuje vybrání určitého rozsahu hodnot pomocí slova *to*. Druhé číslo za slovem *output* definuje na jakou DSCP hodnotou bude předchozí hodnota přepsána. DSCP hodnota 0 označuje neprioritní provoz, který bude mít následně hodnotu AF43 (38 DEC). Hodnotou AF43 je běžně označován velmi prioritní provoz, např. online přenos videa.

Na závěr se ještě musí povolit přepis DSCP hodnot na rozhraní pomocí příkazu *trust dscp override*. [14]

```
[SW1]interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1]trust dscp override
```

```
<S5823C>display qos map-table dscp-dscp
Input DSCP      DSCP
------------------------
0               38
1               1
2               2
3               3
4               4
5               5
6               6
7               7
8               8
9               9
```

Obrázek 4.11: Výpis mapování provozu na hodnotu AF43 pomocí příkazu display qos map-table

4.2.4 Testování mapování provozu na přepínačích Huawei

```
▸ Frame 740: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0
▾ Ethernet II, Src: Performa_00:00:01 (00:10:94:00:00:01), Dst: Performa_00:00:03 (00:10:94:00:00:03)
  ▸ Destination: Performa_00:00:03 (00:10:94:00:00:03)
  ▸ Source: Performa_00:00:01 (00:10:94:00:00:01)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 192.85.1.2, Dst: 192.0.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x98 (DSCP: AF43, ECN: Not-ECT)
    Total Length: 110
    Identification: 0x6f6f (28527)
  ▸ Flags: 0x0000
    Time to live: 255
    Protocol: Unknown (253)
    Header checksum: 0xc932 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.85.1.2
    Destination: 192.0.0.1
▸ Data (90 bytes)
```

Obrázek 4.12: Výpis přeznačkovaného provozu s DSCP: AF43 pomocí dscp-dscp mapy

4.3 Srovnání kompatibility pro přeznačkování a mapování provozu na přepínačích Cisco a Huawei

Přepínače od obou výrobců mají dost podobné příkazy. Z velké části se liší pouze v názvu příkazu. Na přepínačích Cisco musíme vytvořit třídu, ve které definujeme vlastnosti pro výběr provozu a mapu politik, pro kterou nastavíme přeznačkování provozu. U těchto přepínačů musíme navíc přiřadit tuto mapu politik konkrétnímu rozhraní přepínače. U přepínačů Huawei vybíráme provoz přes provozní klasifikaci a dále provoz přeznačkováváme ve třídě provozní chování. Pro tyto přepínače fungují mapy politik globálně na všech portech, kde je povolen přepis

DSCP hodnot.

Chování nástrojů pro přeznačkování provozu jsou totožné, změny jsou pouze v rámci syntaxe na daném zařízení. Přepínače značky Cisco navíc umožňují v rámci nastavení politiky definovat přeznačkování provozu v závislosti na překročení definované průměrné propustnosti. Také jsem testoval změny v přenosové rychlosti při velkém počtu datových toků s maximálním využítím propustnosti rozhraní na 1 Gbit/s. Avšak rychlost byla s velmi malými odchylkami totožná jako rychlost před přeznačkováním. Dospěl jsem tedy k závěru, že přepínače jsou uzpůsobeny na práci přeznačkování s mnoha datovými toky současně.

V rámci druhého nástroje pro mapování jsou příkazy na obou zařízeních syntakticky rozlišné, avšak chovají se stejně. Obě zařízení totožně umožňují využití mnoha mapovacích tabulek podle různých informativních hodnot z hlaviček L2 i L3 vrstev.

4.4 Srovnání možnosti nasazení nástrojů pro přeznačkování a mapování provozu na přepínačích a směrovačích

Přeznačkování provozu je využíváno primárně na směrovačích, ale také přepínačích. Oba přední výrobci mají implementován tento nástroj v rámci přepínačů, viz. praktické srovnání přeznačkování provozu, tak také na svých směrovačích.

V rámci mapování provozu máme na přepínačích více možností než na směrovačích, existuje zde mnoho mapovacích tabulek s různými typy polí pro mapování. Naopak Cisco směrovače nevyužívají nástroj pro mapování a využívají pouze nástroj pro přeznačkování provozu. Směrovače Huawei mají implementovány oba nástroje.

Příkazy jsou téměř totožné, jak na přepínačích, tak také na směrovačích v rámci daného výrobce.

5 Praktická realizace omezování a tvarování provozu

Další testovaný nástroj bude tvarování a omezování provozu. Tvarování provozu funguje tak, že rámce, které by překročili stanovené pásmo, přepínač zařadí do fronty. Datový tok je shlukovitý a nárazový, tudíž jej tvarování rozloží v čase. Tvarování je využito na odchozím rozhraní přepínače.

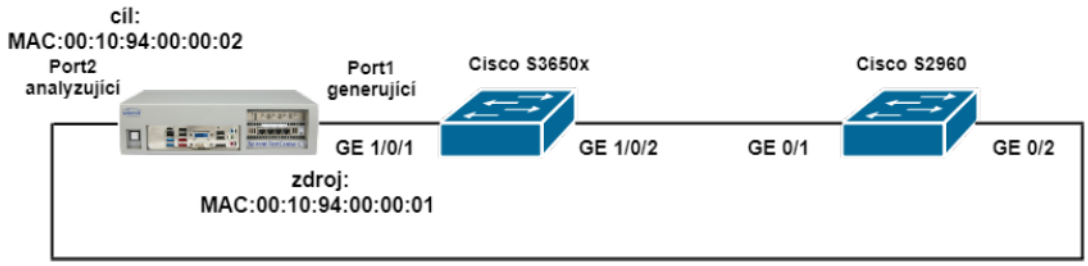
Omezování provozu omezuje provoz tak, že rámce překračující nastavené pásmo zahodí nebo je dále může přeznačkovat. Provoz lze omezit jak na vstupu tak i na výstupu z rozhraní přepínače.

Tvarování a omezování provozu bude aplikováno na vstupním rozhraní přepínače. V rámci této kapitoly budou využity zařízení Cisco S2960/C3650x a Huawei Quidway S2326TP/S5328C.

Do testovací topologie budou vysílány dva datové toky, které budou označeny DSCP hodnotami: EF (46 DEC) pro přenos hlasu a AF13 (14 DEC) pro datový přenos. Na zařízení Spirent je nastaven multistream se dvěma datovými toky s pevným časovým rozptylem. [11][12]

5.1 Omezování provozu

5.1.1 Nastavení omezování provozu na přepínačích Cisco



Obrázek 5.1: Cisco testovací topologie pro omezování provozu

Pro omezení provozu je nejdříve potřeba oba datové toky přiřadit k jednotlivým provozním třídám. Třída s názvem Trida1 bude obsahovat provoz, který je označkován DSCP hodnotou EF a Trida2 bude obsahovat druhý provoz s DSCP hodnotou AF13.

```
SW1(config)#class-map Trida1
SW1(config-cmap)#match ip dscp ef

SW1(config)#class-map Trida2
SW1(config-cmap)#match ip dscp af13
```

Jako druhý krok je nutné přiřadit tyto třídy k mapě politiky s názvem Politika1. V rámci definice Politiky1 určím omezení provozu pro jednotlivé datové toky. Tok s hodnotou EF bude omezován propustností 20 000 kbit/s. V případě navýšení propustnosti toku nedojde k zahození paketů díky nastavení přes příkaz *police* s využitím parametru *transmit*.

Přepínače Cisco využívají obdobný mechanizmus jako přepínače Huawei, využívají také dva kupónové kyblíky, které budou detailněji popsány v další části u zařízení Huawei. Tyto kyblíky mají velikost Burst size (Bc) a Excess Burst size (Be). Mechanizmus může přenést provoz o průměrné propustnosti CIR (Committed Information Rate) a nárazově umožňuje přenést Bc bytů navíc. Provoz je značkován barevně: zeleně, žlutě a červeně. Tento omezovací mechanizmus má tři možnosti jak naložit s daným provozem. Pakety spadající do první možnosti jsou označeny zeleně, pakety spadající do druhé možnosti žlutě a všechen ostatní provoz převyšující obě předchozí možnosti je označen červeně. [14]

- **conform action** - tato akce je vyvolána pro pakety, které odpovídají půměrné propustnosti CIR a normální velikosti shluku (Bc).
- **exceed action** - tato akce je vyvolána pro pakety, které odpovídají půměrné propustnosti CIR + (Bc + Be), popř. propustnosti PIR + Be.
- **violate action** - tato akce je vyvolána pro pakety, které překročí obě předchozí možnosti.

```
SW1(config)#policy-map Politika1
SW1(config-pmap)#class Trida1
SW1(config-pmap-c)#police cir 20000000 pir 100000000 conform-action transmit
exceed-action transmit violate-action transmit

SW1(config-pmap)#class Trida2
SW1(config-pmap-c)#police cir 40000000 conform-action transmit exceed-action drop

SW1(config)#interface gigabitEthernet 1/0/1
SW1(config-if)#service-policy input Politika1
```

Z příkazů lze vidět, že první tok nebude nijak omezován. Druhý datový tok bude omezován, překročí-li průměrnou propustnost 40 000 kbit/s. Tento nadbytečný provoz bude zahazován. Jako poslední krok je nutné tuto politiku aplikovat na vstup rozhraní GE 1/0/1.

5.1.2 Testování omezování provozu na přepínačích Cisco

Provoz byl testován zařízením Spirent TestCenter C1. Zařízení generovalo provoz EF s propustností 500 000 kbit/s a provoz AF13 s propustností 500 000 kbit/s. Celkem tedy přístroj generoval dva datové toky s celkovou propustností 1 000 Mbit/s. Níže jsou uvedeny souhrnné údaje k oběma portům zařízení. Ve výpisu 5.3 jsou důležité položky **Port Tx L1 (bit/s)** a **Port Rx L1 (bit/s)**.

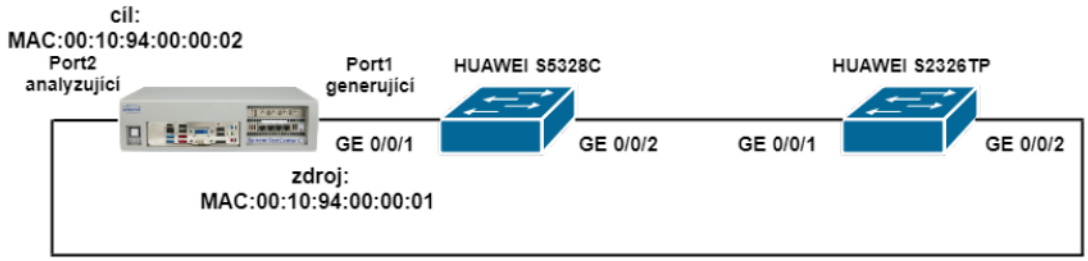
	☑	StreamBlock 3-2(EF)	Click to ad...	*Ready*	*1*	500,000,000	bps
	☑	StreamBlock 6-2(AF13)	Click to ad...	*Ready*	*1*	500,000,000	bps

Obrázek 5.2: Cisco statistiky datových proudů - bez omezení provozu

Port Name	Port Tx L1 Rate (bps)	Port Rx L1 Rate (bps)	Port Tx L1 Rate (Percent)	Port Rx L1 Rate (Percent)	Port Min Latency (us)	Port Max Latency (us)
Port //1/1 (offline)	999999907	0	99,9999907	0		
Port //1/2 (offline)	0	53996085	0	5,3996085	12,51	4516,62

Obrázek 5.3: Cisco statistiky datových proudů s omezením provozu

5.1.3 Nastavení omezování provozu na přepínačích Huawei



Obrázek 5.4: Huawei testovací topologie pro omezování provozu

Nejprve je nutné datové toky rozlišit podle hodnoty DSCP a přidělit je jednotlivě k provozním třídám. Přidělení datového toku k dané třídě je zaručeno pomocí příkazu *if-match dscp value*. Provozní třída Trida1 bude obsahovat provoz označený DSCP hodnotou EF a Trida2 provoz označený hodnotou AF13.

```
[SW1] traffic classifier Trida1
[SW1-classifier-Trida1] if-match dscp ef

[SW1] traffic classifier Trida2
[SW1-classifier-Trida2] if-match dscp af13
```

Níže nastavím chování jednotlivých provozních tříd. Třídy budou k jednotlivým chováním přiděleny později.

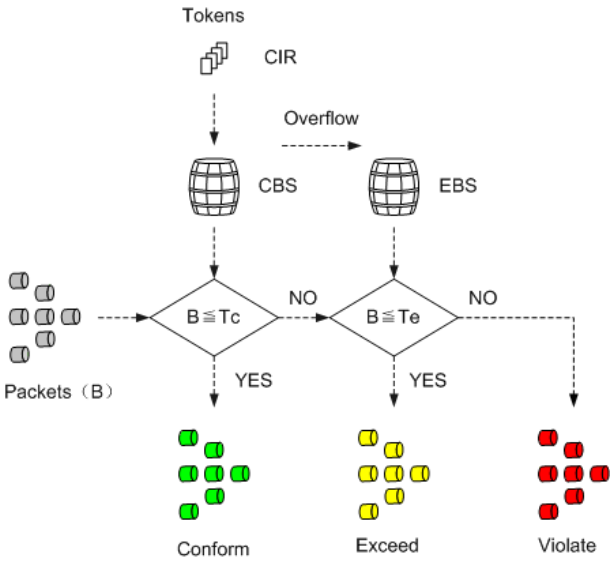
Přepínače Huawei pracují stejně jako přepínače Cisco s algoritmem zvaným kupónový kyblík (Token Bucket). Do kyblíku se přidávají kupóny (tokens) průměrnou přenosovou propustností (CIR - Committed Information Rate). Tento kyblík má omezenou velikost Bc (Burst size), pokud je plný, tak se příchozí provoz zahazuje. V případě příchodu paketu budou z kyblíku odebrány kupóny (1 kupón = 1 byte paketu) a provede se odeslání dat. V případě nedostatku kupónů je paket zahozen. [15][16]

```
[SW1] traffic behavior Chov1
[SW1-behavior-Chov1] car cir 20000 pir 100000 green pass yellow pass red pass
[SW1-behavior-Chov1] statistic enable

[SW1] traffic behavior Chov2
[SW1-behavior-Chov2] car cir 40000 green pass yellow discard red discard
[SW1-behavior-Chov2] statistic enable
```

Tato zařízení využívají nástroj CAR. Tento nástroj využívá dva kupónové kyblíky (Token Bucket), kyblík C a P. Kyblík C je doplňován kupóny propustností (CIR - Committed Information Rate) a má maximální velikost CBS (Commited Burst Size). Kyblík P je doplňován kupóny maximální povolenou propustností (PIR - Peak Information Rate) a má maximální velikost EBS (Excess Burst Size), viz. schéma funkčnosti kyblíků 5.5.

V případě, že na přepínač dorazí provoz s propustností B a kyblík C má dostatek tokenů, jsou pakety označeny zeleně. Pokud kyblík C má dostatek kupónů přo přenos paketů, ale kyblík P nikoliv, jsou pakety označeny žlutě. V ostatních případěch jsou pakety označeny červeně. [15][16]

Dále je nutné vytvořit provozní politiku, ve které propojím obě třídy k třídám chování. Posledním příkazem aplikuji tuto politiku na vstup rozhraní GE 0/0/1.



Obrázek 5.5: Kyblíky tokenů Huawei [15]

```
[SW1] traffic policy Politika1
[SW1-trafficpolicy-p1] classifier Trida1 behavior Chov1
[SW1-trafficpolicy-p1] classifier Trida2 behavior Chov2

[SW1] interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] traffic-policy Politika1 inbound
```

5.1.4 Testování omezování provozu na přepínačích Huawei

Ověřit nastavení provozních tříd lze příkazem *display traffic classifier* a politik nastavených na přepínači pomocí příkazu *display traffic behavior user-defined*. [13]

```
[SW1] display traffic classifier user-defined
[SW1] display traffic behavior user-defined
```

Dále byl provoz otestován zařízením Spirent TestCenter C1. Zařízení generovalo provoz EF s propustností 500 000 kbit/s a provoz AF13 s propustností 500 000 kbit/s. Celkem tedy přístroj generoval dva datové toky s celkovou propustností 1 000 Mbit/s. Níže jsou uvedeny souhrnné údaje k oběma portům zařízení. Ve výpisu 5.9 jsou důležité položky **Port Tx L1 (bit/s)** a **Port Rx L1 (bit/s)**.

```
[S5328TP]display traffic behavior user-defined
  User Defined Behavior Information:
    Behavior: Chov1
      Committed Access Rate:
        CIR 20000 (Kbps), CBS 2500000 (Byte)
        PIR 100000 (Kbps), PBS 12500000 (Byte)
        Green Action   : pass
        Yellow Action  : pass
        Red Action     : pass
      Statistic: enable
    Behavior: Chov2
      Committed Access Rate:
        CIR 40000 (Kbps), CBS 5000000 (Byte)
        PIR 40000 (Kbps), PBS 5000000 (Byte)
        Green Action   : pass
        Yellow Action  : discard
        Red Action     : discard
      Statistic: enable

Total behavior number is 2
```

Obrázek 5.6: Výpis tříd chování: behavior user-defined

	☑	StreamBlock 3-2(EF)	Click to ad...	*Ready*	*1*	500,000,000	bps
	☑	StreamBlock 6-2(AF13)	Click to ad...	*Ready*	*1*	500,000,000	bps

Obrázek 5.7: Huawei statistiky datových proudů bez omezení provozu

Name/ID	Tx L1 Rate (bps)	Rx L1 Rate (bps)
StreamBlock 1-2(CS7)/98304	*0*	*0*
StreamBlock 6-2(AF13)/98306	*499,999,804*	*40,000,577*
StreamBlock 3-2(EF)/98305	*499,999,848*	*500,000,166*

Obrázek 5.8: Huawei statistiky datových proudů s omezení provozu

Port Name	Port Tx L1 Rate (bps)	Port Rx L1 Rate (bps)	Port Tx L1 Rate (Percent)	Port Rx L1 Rate (Percent)	Port Min Latency (us)	Port Max Latency (us)
Port //1/1 (offline)	999999912	0	99,9999912	0		
Port //1/2 (offline)	0	540000554	0	54,0000554	6,01	8,44

Obrázek 5.9: Huawei statistiky datových proudů na portech generátoru s omezením provozu

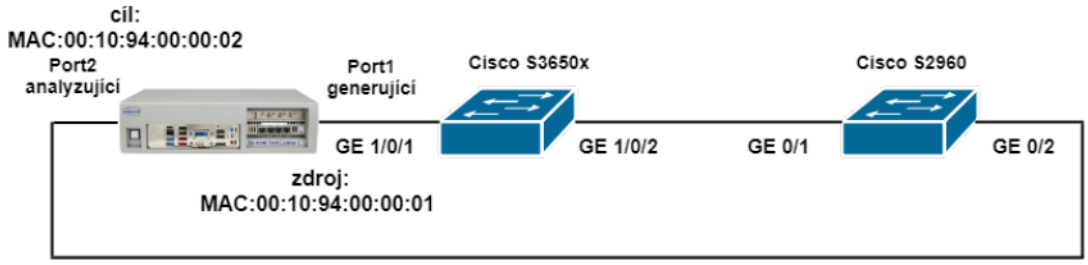
Níže je uveden výpis po zadání příkazu *display traffic policy statistics*. Slouží pro ověření, že mechanizmus CAR skutečně zahazoval provoz, který byl nad stanovenou propustnost 20 000 kbit/s.

```
[S5328TP]display traffic policy statistics interface GigabitEthernet 0/0/1 inbound

 Interface: GigabitEthernet0/0/1
 Traffic policy inbound: Politika1
 Rule number: 2
 Current status: OK!
 Statistics interval: 300
-----------------------------------------------------------------------
 Board : 0
-----------------------------------------------------------------------
 Matched          |      Packets:                  398,374,853
                  |      Bytes:                              -
                  |      Rate(pps):                  845,061
                  |      Rate(bps):                          -
-----------------------------------------------------------------------
   Passed         |      Packets:                  215,155,383
                  |      Bytes:                              -
                  |      Rate(pps):                  456,333
                  |      Rate(bps):                          -
-----------------------------------------------------------------------
   Dropped        |      Packets:                  183,219,470
                  |      Bytes:                              -
                  |      Rate(pps):                  388,728
                  |      Rate(bps):                          -
-----------------------------------------------------------------------
     Filter       |      Packets:                            0
                  |      Bytes:                              -
-----------------------------------------------------------------------
     Car          |      Packets:                  183,219,470
                  |      Bytes:                              -
-----------------------------------------------------------------------
```

Obrázek 5.10: Výpis provozních politik (CAR)

5.2 Tvarování provozu

5.2.1 Nastavení tvarování provozu na přepínačích Cisco



Obrázek 5.11: Cisco testovací topologie pro tvarování provozu

Na přepínačích Cisco lze tvarovat provoz buď globálně přes příkaz *traffic-shape* nebo pomocí definování provozu pomocí hodnot DSCP. Tvarování provozu jsem provedl pomocí politiky na obou datových proudech na propustnost 20 000 kbit/s a aplikoval jej na výchozí rozhraní GE 1/0/1. Toto tvarování provozu funguje na principu časového rozložení provozu s využitím vyrovnávací paměti rozhraní (buffer), viz. popis v předchozí teoretické části 2.2.3. Provoz tedy není zahazován.

```
SW1(config)#class-map Trida3
SW1(config-cmap)#match dscp ef af13

SW1(config)#policy-map Politika2
SW1(config-pmap)#class Trida3
SW1(config-pmap-c)#shape average 20000000

SW1(config)#interface gigabitEthernet 1/0/1
SW1(config-if)#service-policy output Politika2
```

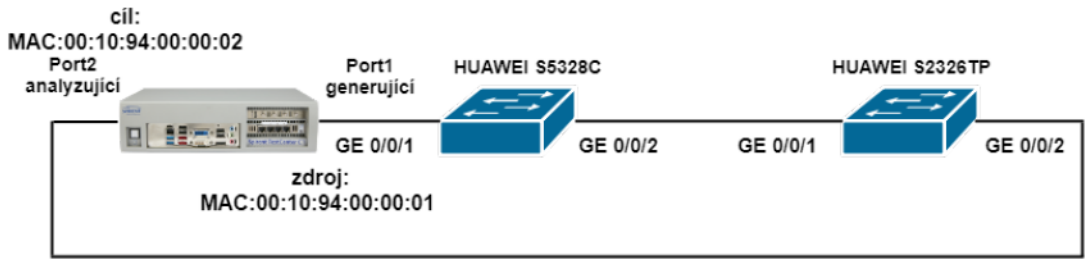
5.2.2 Testování tvarování provozu na přepínačích Cisco

Tvarování provozu bylo testováno na obou datových proudech, které nebyly nijak omezovány předchozím nastavením přepínače. Provoz na výchozím rozhraní GE 1/0/2 byl nastavením tvarován na propustnost 20 000 kbit/s.

Port Name	Port Tx L1 Rate (bps)	Port Rx L1 Rate (bps)	Port Tx L1 Rate (Percent)	Port Rx L1 Rate (Percent)	Port Min Latency (us)	Port Max Latency (us)
Port //1/1 (offline)	999999967	0	99,9999967	0		
Port //1/2 (offline)	0	19900474	0	1,9900474	13,11	31909,09

Obrázek 5.12: Cisco statistiky datových proudů s omezením provozu

5.2.3 Nastavení tvarování provozu na přepínačích Huawei



Obrázek 5.13: Huawei testovací topologie pro tvarování provozu

Na výchozím rohraní GE 0/0/2 prvního přepínače bylo aplikováno tvarování provozu. Provoz bude tvarován s propustností 20 000 kbit/s.

```
[SW1] interface GigabitEthernet 0/0/2
[SW1-Ethernet0/0/2] qos lr outbound cir 20000
```

5.2.4 Testování tvarování provozu na přepínačích Huawei

Nastavení pro testování tvarování provozu bylo totožné. Bylo využito totožné schéma zapojení všech zařízeních. Tvarování provozu bylo testováno na obou datových proudech, které nebyly nijak omezovány předchozím nastavení přepínače. Provoz na výchozím rozhraní GE 0/0/2 byl nastavením tvarován na propustnost 20 000 kbit/s.

Port Name	Port Tx L1 Rate (bps)	Port Rx L1 Rate (bps)	Port Tx L1 Rate (Percent)	Port Rx L1 Rate (Percent)	Port Min Latency (us)	Port Max Latency (us)
Port //1/1 (offline)	1000000129	0	100,0000129	0		
Port //1/2 (offline)	0	20032304	0	2,0032304	46104,01	61535,28

Obrázek 5.14: Huawei statistiky datových proudů s tvarováním provozu

5.3 Srovnání kompatibility pro omezování a tvarování provozu na přepínačích Cisco a Huawei

Přepínače od obou výrobců mají podobné příkazy. Z velké části se liší pouze v názvu příkazu. Na přepínačích Cisco musíme opět vytvořit třídu, ve které definujeme vlastnosti pro výběr provozu, který chceme následně omezovat. Omezení provádíme již v samotném nastavení mapy politik. V rámci přepínačů Cisco musíme propustnosti k jednotlivým datovým tokům definovat v jednotkách bit/s. U přepínačů Huawei vybíráme tento provoz v rámci pravidel (Traffic classifier) a provoz omezujeme pomocí pravidel (Traffic behavior). V rámci pravidel (Traffic classifier) musíme definovat datové toky s propustnostmi v jednotkách kbit/s.

Chování nástrojů pro omezování a tvarování provozu jsou totožné. Přepínače Cisco C3650x mají k dispozici 12MB výstupní paměť (buffer) pro všechny porty v rámci tvarování provozu. Modely S2960 pouze 4MB vyrovnávací paměť. Přepínače Huawei S2326TP/S5329TP mají pouze 2.5MB výstupní paměť pro všechny porty v rámci tvarování provozu. Velikost paměti na přepínačích Cisco musíme nastavovat v rámci mapy politik příkazem *queue-limit (number-of-packets, 1 to 64)*. Tuto velikost na přepínači Huawei lze v rámci portu nastavit příkazem *qos queue number-of-queue length (0 - 1 134 208 bits)*.

5.4 Srovnání možnosti nasazení nástrojů pro omezování a tvarování provozu na přepínačích a směrovačích

Tvarování a omezování provozu je primárně využíváno na směrovačích v rámci ISP poskytovatele připojení k internetu. Kdy zákazníkům poskytovatel garantuje určitou propustnost a nadlimitní data buď úplně zahazuje nebo časově rozloží pomocí tvarování provozu. Avšak díky stále rostoucím sítím je nutno tyto nástroje aplikovat již v rámci LAN sítí. Nižší modely přepínačů neumožňují tvarování provozu, využívají pouze omezování provozu.

Na vyšších modelech přepínačů je možnost vytvářet více policerů (omezovačů provozu): Individuální a Agregované omezovače. V rámci individuálního omezovače musíme omezení propustnosti nastavovat zvlášť pro každou třídu provozu. Avšak v rámci agregovaného omezovače omezujeme propustnost celkově na všechny potřebné datové toky. Vytváříme omezovač a ten využíváme uvnitř několika provozních map.

6 Praktická realizace priorizace provozu

Posledním testovaným nástrojem bude priorizace provozu pomocí různých typů CoS hodnot. Na každém zařízení existuje těchto 8 CoS front, zde je jejich výčet: |BE | AF1 | AF2 | AF3 | AF4 | EF | CS6 | CS7|. Do testovací topologie budou vysílány tři datové toky, které budou označeny DSCP hodnotami: CS7 (56 DEC) pro přenos videa, AF13 (14 DEC) pro datový přenos a EF (46 DEC) pro přenos hlasu.

Typy metod obsluhy front přepínače Huawei Quidway S2326TP/S5329C a Cisco S2960/C3650x

Obě zařízení mají podobné varianty obsluhy front. Přepínač Huawei S2326TP primárně využívá obsluhu front nazvanou **WRR** (Weighted Round Robin) a **DRR** (Deficit Round Robin). Round Robin znamená v jednoduchosti to, že z výstupních front se postupně odebírají pakety. Pomocí vah zajistíme jednotlivým frontám proporcionální obsloužení podle dané váhy. Jednotlivými váhami definujeme propustnost, která je založena na počtu přenesených paketů na rozdíl od metody DRR, kdy je metoda obsluhy založena na počtu přenesených bajtů. Využívá se také možnost obsluhy **SP+WRR**, která je doplněná o striktní frontu, která je obluhována do doby dokud není zcela prázdná. A až poté jsou obsluhovány fronty s metodou WRR.

Jako druhou možnost využívá obsluhu fronty **SP** (Strict Priority). Tato fronta funguje na principu priorit, nejprve jsou obsluhovány fronty s vyšší prioritou a až poté fronty s prioritou nižší. Nevýhoda tohoto řešení spočívá v tom, že dokud nebudou fronty s vyšší prioritou prázdné k ostatním méně prioritním frontám se nedojde.[1][6][14]

Přepínač Cisco S2960 využívá v rámci priorizace primárně obsluhu fronty typu **SRR** (Shape/Shared Round Robin). Jedná se o technologické vylepšení obsluhy WRR. WRR plánovač je zde nahrazen plánovačem SRR. SRR může pracovat buď v módu Shared nebo Shaped. Je využita zahazovací strategie WTD (Weighted Tail Drop), využívá tři prahové hodnoty. První dvě lze upravit, třetí je fixní na 100 %. WTD oproti mechanizmu TD (Tail Drop) zahazuje provoz před překročení určitého nastaveného prahu. Přepínač S2960 využívá dvě vstupní SRR fronty a čtyři výstupní SRR fronty.[1][2][6][10]

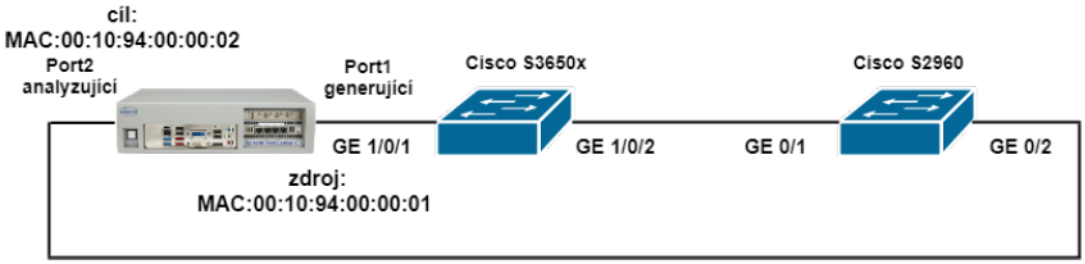
Jako sekundární metodu obsluhy front využívá obsluhu fronty typu **PQ** (Priority Queuing), která byla popsána již v kapitole 2.2.2 . Svou funkčností je velmi podobná dříve zmiňované obsluze fronty SP. Obsluha PQ využívá 4 typy front s nastavenými prioritami: High, Medium, Normal a Low.

Tabulka 6.1: Srovnání front u Huawei a Cisco přepínačů

Huawei	Cisco
SP	PQ
WRR SP+WRR	SRR
DRR SP+DRR	

6.1 Priorizace provozu

6.1.1 Nastavení priorizace provozu na přepínačích Cisco



Obrázek 6.1: Cisco testovací topologie pro priorizaci provozu

Pro priorizaci provozu je nutné nejprve přiřadit všechny datové provozy k provozním třídám. Třída Video bude obsahovat provoz označkovaný DSCP hodnotou CS7, třída Hlas bude obsahovat provoz označkován hodnotou EF a třída Data bude obsahovat poslední provoz s hodnotou AF13. Každý jednotlivý provoz je generován s propustností 333.33 Mbit/s.

```
SW1(config)#class-map Video
SW1(config-cmap)#match ip dscp cs7

SW1(config)#class-map Hlas
SW1(config-cmap)#match ip dscp ef

SW1(config)#class-map Data
SW1(config-cmap)#match ip dscp af13
```

Dále je nutné přiřadit tyto jednotlivé třídy k mapě politik s názvem Fronty. Zde je jednotlivým provozům přiřazena procentuálně propustnost vztažená k celkové propustnosti portu. Port je ve výchozím stavu nastaven na maximální propustnost 1 Gbit/s, tato propustnost je z důvodu testování níže snížena na desetinu, tedy 100 Mbit/s, aby byl přepínač donucen k priorizaci provozu.

```
SW1(config)#policy-map Fronty

SW1(config-pmap)#class Video
SW1(config-pmap-c)#bandwidth percent 40

SW1(config-pmap)#class Hlas
SW1(config-pmap-c)#bandwidth percent 35

SW1(config-pmap)#class Data
SW1(config-pmap-c)#bandwidth percent 25

SW1(config)#interface gigabitEthernet 1/0/1
SW1(config-if)#service-policy output Fronty
SW1(config-if)#speed 100
```

Přepínač Cisco S3650x má QoS vlastnosti již ve výchozím stavu povoleny, jelikož se jedná o L3 přepínač. Proto se zde nemusí povolat funkce MLS QoS ani důvěru v DSCP hodnoty.

6.1.2 Testování priorizace provozu na přepínačích Cisco

Každému ze tří datových toků byla přidělena třetina propustnosti rozhraní. Níže jsou zobrazeny propustnosti vztažené k jednotlivým datovým tokům.

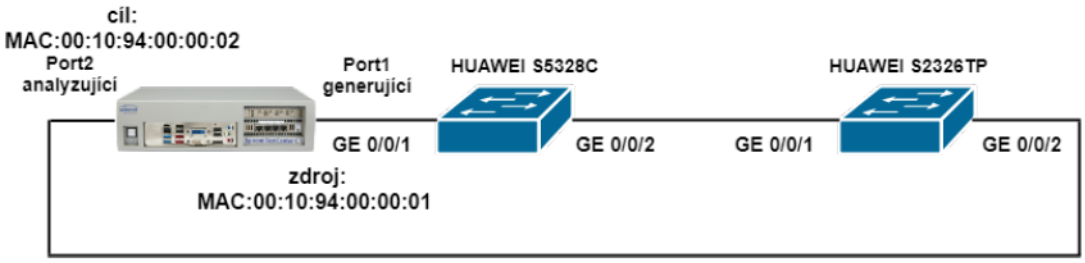
Datový tok označený DSCP hodnotou CS7 měl propustnost 40 000 kbit/s, EF tok měl propustnost 35 000 kbit/s a poslední AF13 tok měl propustnost 25 000 kbit/s. Celková propustnost rozhraní byla nastavena na hodnotu 100 000 kbit/s.

Jak je zřetelené z výpisu, priorizace provozu funguje podle očekávání. Z výsledků lze vidět menší nepřesnosti v propustnostech jednotlivých datových toků. Tyto malé nepřesnosti mohou být způsobeny měřícím přístrojem nebo daným přepínačem.

Tx Port	Rx Port	Stream Block	Stream Id	Stream Index	Port Tx L1 Rate (bps)	Port Rx L1 Rate (bps)
Port //1/1	Port //1/2	StreamBlock 1-2(CS7)	98304	32768	333 333 334	39 966 097
Port //1/1	Port //1/2	StreamBlock 3-2(EF)	98305	32769	333 333 318	35 057 630
Port //1/1	Port //1/2	StreamBlock 6-2(AF13)	98306	32770	333 333 309	24 978 374

Obrázek 6.2: Cisco statistiky datových proudů s priorizací provozu

6.1.3 Nastavení priorizace provozu na přepínačích Huawei



Obrázek 6.3: Huawei testovací topologie pro priorizaci provozu

Přepínač Huawei obsahuje na každém rozhraní 8 front, které jsou namapovány na 8 CoS hodnot: |BE | AF1 | AF2 | AF3 | AF4 | EF | CS6 | CS7|. Na přepínači lze zvolit, zda se má využít vlastnosti WRR/WRR+SP nebo DRR/DRR+SP. Zvolil jsem metodu WRR, v případě využití hodnoty 0 pro parametr weight bude fronta využívat vlastnosti SP. V tomto případě by měla tato fronta nejvyšší prioritu oproti ostatním frontám s nenulovými hodnotami weight. Dále je nutné na rozhraních povolit důvěru v DSCP hodnoty.

```
[SW1] interface Gigabitethernet 0/0/1
[SW1-GigabitEthernet0/0/1] qos wrr
[SW1-GigabitEthernet0/0/1] qos queue 7 wrr weight 40
[SW1-GigabitEthernet0/0/1] qos queue 5 wrr weight 35
[SW1-GigabitEthernet0/0/1] qos queue 1 wrr weight 25
[SW1-GigabitEthernet0/0/1] trust dscp

[SW1-GigabitEthernet0/0/1] undo negotiation auto
[SW1-GigabitEthernet0/0/1] speed 100

[SW1] interface Gigabitethernet 0/0/2
[SW1-GigabitEthernet0/0/2] trust dscp
```

6.1.4 Testování priorizace provozu na přepínačích Huawei

Stejně jako v předchozím případě byla každému toku nastavena třetina propustnosti rozhraní.

Datové toky měli rozděleno pásmo propustnosti ve stejném poměru, jako u přepínačů Cisco a to v poměru 40 : 35 : 25 % celkové propustnosti rozhraní. I zde jsou vidět menší nepřesnosti v propustnostech, avšak jsou mírně vyšší než v případě přepínačů Cisco. Tyto nepřesti jsou způsobeny přepínači a měřícím přístrojem.

Tx Port	Rx Port	Stream Block	Stream Id	Stream Index	Port Tx L1 Rate (bps)	Port Rx L1 Rate (bps)
Port //1/1	Port //1/2	StreamBlock 1-2(CS7)	98304	32768	333 333 419	39 640 522
Port //1/1	Port //1/2	StreamBlock 3-2(EF)	98305	32769	333 333 215	34 666 699
Port //1/1	Port //1/2	StreamBlock 6-2(AF13)	98306	32770	333 333 478	24 771 202

Obrázek 6.4: Huawei statistiky datových proudů s priorizací provozu

6.2 Srovnání kompatibility příkazů pro priorizaci provozu na přepínačích Cisco a Huawei

Základní rozdílnost je již v rozdílné konfiguraci. Kdy v případě přepínačů Cisco jsem využil SRR metodu a v rámci Huawei metodu WRR. Tyto oba přístupy jsou takřka totožné. Metoda WRR využívá mechanizmus MTD (Modified Tail Drop) obdoba mechanizmu WTD (Weighted Tail Drop) na Cisco zařízeních. Provoz zahazuje dříve než dosáhne nastaveného prahu. SRR metoda využívá mechanizmus WTD. V rámci Cisco přepínačů volíme pro každý provoz procentuální propustnost pro danou frontu. Avšak u konkurenčních přepínačů se pracuje s váhami, které se sečtou a propustnost daného portu je průměrově rozdělena těmto váhám.

6.3 Srovnání možnosti nasazení nástrojů pro priorizace provozu na přepínačích a směrovačích

Priorizace provozu je primárně využívána na PHB (hraničních) směrovačích. Zde je hlavním identifikátorem pro QoS mechanizmy DSCP pole, které umožňuje využít až 64 tříd. Priorizace na přepínačích využívá identifikátor CoS (Class of Service) v hlavičce rámce, který umožňuje využití až 8 tříd. L3 přepínače umí také pracovat s polem DSCP z hlavičky paketu, jako již zmíněné směrovače.

Hlavní rozdíl mezi těmito zařízeními je v možnostech typů obsluhy front. Nižší a střední modely přepínačů využívají základní typy obsluhy front jako je SP (Strict Priority), WRR (Weighted Round Robin) popř. její alternativa SRR (Shape Round Robin). Směrovače mají více možností těchto metod např. navíc využívají metody WFQ (Weighted Fair Queuing) a LLQ (Low-Latency Queuing).

Metoda WFQ umožňuje využití mnohonásobně většího množství výstupních front než metody WRR a SRR, proto je tento přístup využit na výkonnějších zařízeních jako jsou směrovače. LLQ je vylepšení CBWFQ s jednou prioritní frontou. Během cyklu výběru z front, se vždy mezi výběry z jednotlivých front odebere z prioritní fronty jeden paket.

Závěr

Cílem mé bakalářské práce bylo srovnání a realizace nástrojů pro kvalitu služby na přepínačích Cisco a Huawei. Využitá zařízení podporovala nástroje pro přeznačkování a mapování provozu, omezování a tvarování provozu a priorizaci provozu. Každý nástroj byl vybírán tak, aby fungoval na přepínači Cisco i na přepínači Huawei. Vybraná řešení využívají velmi podobné konfigurační postupy.

Jako první byly vybrány nástroje pro přeznačkování a mapování provozu. Nástroj pro přeznačkování provozu byl svou funkčností totožný na obou zařízeních. Přepínač Cisco navíc oproti přepínači Huawei umožňuje využít speciální police-dscp-transmit mapu, která je využívána při překročení nastavené propustnosti označkovaného datového provozu v nastavení přepínače. Dojde-li k překročení nastavené propustnosti, nastane přeznačkování provozu na DSCP hodnotu 0x00 hexadecimálně. Při druhém nástroji pro mapování provozu, byla v obou případech využita DSCP mapa, která prováděla změnu DSCP hodnoty rámce podle nastavené konfigurace.

Nástroje pro omezování a tvarování provozu fungovaly na obou zařízeních zcela totožně. Omezování i tvarování provozu probíhalo s vysokou přesností nastavených propustností jednotlivých datových toků. Mírně přesnější hodnoty propustností měly přepínače firmy Huawei. Základní odlišnost obou řešení byla pouze v jednotkách, ve kterých se definovala propustnost pro omezování datových toků. Cisco přepínače vyžadují definici propustností v jednotkách bit/s a přepínače Huawei v jednotkách kbit/s.

Posledním testovaným byl nástroj pro priorizaci provozu. Základní odlišnost obou řešení byla v použití metod obsluhy front. Přepínače firmy Huawei využívají metodu WRR (Weighted Round Robin) a přepínače Cisco využívají vylepšenou metodu SRR (Shared Round Robin). Metoda SRR využívá plánovač Shared. Tento plánovač rozdělí kolo obsluhy front na minikola, kdy přepínač rozhoduje, zda odeslat jeden paket nebo žádný. Při této metodě obsluhy front přepínač neodesílá větší počet paketů než jeden. Obě metody využívají váhy při konfiguraci.

Při konfiguraci nástrojů na přepínačích obou výrobců lze vidět podobnost v použité syntaxi. Například příkaz *match* u přepínačů Cisco a *if-match* u přepínačů Huawei. Pro přiřazení politik na rozhraní se na přepínačích Cisco využívá příkaz *service-policy input <název>* a na přepínačích Huawei příkaz *traffic-policy <název> inbound*. Přepínače Huawei navíc umožňují využít užitečný příkaz na zobrazení celkových statistik na rozhraní. Tyto statistiky lze zobrazit pomocí příkazu *display this*.

Dále lze bakalářskou práci rozšířit o téma kvality služby v sítích s využitím technologie MPLS, případně MPLS VPN. Bylo by zajímavé propojit síť využívající technologii Ethernet se sítí s technologií MPLS a zde otestovat chování přemapování mezi těmito technologiemi. Porovnat možnosti přeznačkování paketů s různou délkou značkovacích polí s využitím DSCP/CoS a

Experimental hodnot. Technologie MPLS využívá tříbitové experimentální pole, které odpovídá CoS poli v Ethernet rámci. Mimo jiné lze také podrobněji zpracovat více typů obsluhy front. K této konfiguraci by bylo nutné využít vyšší řady přepínačů nebo klasické směrovače obou firem.

Hlavní přínos mé bakalářské práce je v otestování a porovnání rozdílů ve funkčnostech nastavení nástrojů pro kvalitu služby s využitím přepínačů Cisco a Huawei. Tyto nástroje jsou zde detailně popsány, včetně ověření funkčnosti.

Literatura

[1] Cisco DQOS exam certification guide: IP telephony self-study. 2004. Indianapolis, IN: Cisco Press, c2004, s. 44. ISBN 1-58720-058-9.

[2] SZIGETI, Tim, Christina HATTINGH, Robert BARTON a Kenneth BRILEY. End-to-end QoS network design [online]. 2nd edition. Indianapolis, IN: Cisco Press, [2014] [cit. 2018-11-05]. Cisco Press networking technology series. ISBN 15-871-4369-0.

[3] BARZ, Hans W a Gregory A BASSETT. Multimedia networks: protocols, design, and applications. West Sussex: Wiley, 2016. ISBN 978-1-119-09013-7.

[4] ODOM, Wendell, Michael J CAVANAUGH a Wendell ODOM. Cisco QOS exam certification guide: IP telephony self-study. 2nd ed. Indianapolis, IN: Cisco, c2005. ISBN ISBN978-1-58720-124-0.

[5] Quality of Service (QoS) [online]. [cit. 2018-10-21]. Dostupné z: https://www.techopedia.com/definition/9049/quality-of-service

[6] Cisco Qos 1 [online]. 18.01.2009 [cit. 2018-10-21]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-qos-1-uvod-do-quality-of-service-a-diffserv/

[7] GRYGÁREK, Petr. FEI VŠB-TU OSTRAVA. Podpora multimediálních aplikací v Internetu. Ostrava, [cit.2018-11-26]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/multimedia-ucitele.pdf

[8] 802.1Q-2014 - Bridges and Bridged Networks. In: Http://www.ieee802.org [online]. 19th Dec 2014 [cit. 2018-12-13]. Dostupné z: http://www.ieee802.org/1/pages/802.1Q-2014.html

[9] Luc De Ghein. MPLS and Quality of Service Cisco Press [online]. 27 April 2007 [cit. 2018-12-13]. Dostupné z: https://www.networkworld.com/article/2298533/lan-wan/mpls-and-quality-of-service.html

[10] Spirent Test Center : C1. Digital Instrument [online]. [cit. 2019-01-28]. Dostupné z: http://www.digitalinstrument.co.th/spirent-test-centerc1-100192.product

[11] Catalyst 3560 Switch Software Configuration Guide, Release 12.2(55)SE [online]. 2016 [cit.2018-11-07].Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_55_se/configuration/guide/3560_scg/SwCfgIX.html

[12] Catalyst 2960 Switch Software Configuration Guide [online]. 2007 [cit. 2018-11-07]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_40_se/configuration/guide/scg.pdf

[13] S2350, S5300, S6300 V200R003(C00, and C02) Typical Configuration Examples [online]. In: 2013 [cit. 2019-01-28]. Dostupné z: https://support.huawei.com/enterprise/en/doc/EDOC1000027253?idPath=7919710%7C21782164%7C21782167%7C22318553%7C16561

[14] Cisco QoS 3 - omezování rychlosti - Policing, Shaping [online]. In: . [cit. 2019-02-10]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-qos-3-omezovani-rychlosti-policing-shaping/

[15] Traffic Policing, Traffic Shaping, and Interface-based Rate Limiting. In: Http://support.huawei.com [online]. [cit. 2019-02-10]. Dostupné z: http://support.huawei.com/enterprise/docinforeader!loadDocument1.action?contentId=DOC1000069480&partNo=10072

[16] SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

[17] In: Http://www.netcontractor.pl/ [online]. [cit. 2019-02-04]. Dostupné z: http://www.netcontractor.pl/blog/wp-content/uploads/2011/11/QoS-Values-Calculator-v3.jpg

[18] DSCP and Precedence Values [online]. [cit. 2018-11-07]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/sw/4_0/qos/configuration/guide/nexus1000v_qos/qos_6dscp_val.pdf

Přílohy

VII. Popis prostředí programu Spirent TestCenter Application 4.86

VIII. Tabulka pro přepočet CoS a DSCP hodnot

IX. Tabulka pro přepočet 802.1p na DSCP hodnoty

X. Konfigurační soubory pro přeznačkování a mapování provozu

XI. Konfigurační soubory pro omezování a tvarování provozu

XII. Konfigurační soubory pro priorizaci provozu